ABSTRACT

A system and method is disclosed for protecting extensible firmware interface (EFI) runtime services utilizing virtualization technology. The runtime services used by an operating system (OS) are executed by a runtime services monitor (RSM) rather than the operating system itself. When the OS accesses a runtime service, the processor mode automatically switches context to the RSM, which then executes the runtime service and puts the results back in a shared memory location. Virtualization technology is used to effect the automatic context switching. Other embodiments as described and claimed above are disclosed.